IN THE CLAIMS:

Please amend the claims as set forth below:

1. (Currently Amended) A method ~~of~~ for verifying the validity of ~~generating~~ an encrypted code generated in base L, comprising the steps of:

obtaining an encrypted code fashioned as a base L string derived from ~~providing~~ an n-bit raw number by ~~;~~

producing a first string through application of~~applying~~ a one-way hash function ~~on~~ to the n-bit raw number with a first secret key, ~~to generate a first strung;~~

designating an m-bit portion of the first string as an m-bit validation number, ~~; and~~

producing a second string through combination of ~~combining~~ the m-bit validation number and the n-bit raw number ~~to generate a second string~~, producing a third string through application of an encryption algorithm to the second string with a second secret key, and converting the third string to the base L string;

converting the base L string to a base 2 string;

decrypting the base 2 string; and

verifying the validity of the encrypted code by processing the decrypted base 2 string.

2. (Currently Amended) The method of claim 1, ~~further comprisingthe steps~~ wherein the encryption algorithm is ~~of:~~

~~aaplying~~ a DES3 encryption algorithm ~~to the second string with a second secret key to generate a third string; and~~

~~converting the third string to base L to generate the encrypted code~~.

3. (Original) The method of claim 1, wherein n=32, m=16, and L=29.

4. (Original) The method of claim 1, wherein the one-way hash function is MD5.

5. (Currently Amended) The method of claim 1, wherein the combination step ~~of combining~~ includes concatenating the m-bit validation number and the n-bit raw number.

6. (Original) The method of claim 1, wherein the m-bit validation number is the m most significant bit (MSB) portion of the second string.

7. (Currently Amended) The method of claim 1, wherein the m-bit validation number is the m most significant bit (MSB) portion of the first string.

8. (Currently Amended) A method of verifying the ~~valifdity~~ validity of a code obtained by a user from an object, comprising the steps of:

~~generating a code with encrypted information;~~

~~fixing the code on an object to be distributed to a user;~~

~~obtaining the code from the object, by the user;~~

receiving the code ~~on-line~~on-line from the user, the code is generated with encrypted information as a base L string and obtained by the user off-line from the object;

converting the base L string to a base 2 string;

decrypting the base 2 string; and

verifying the validity of the code by processing the ~~encrypted information~~decrypted base 2 string.

9. (Currently Amended) The method of claim 8, wherein the code is generated by~~step of generating includes the steps of~~:

providing an n-bit raw number;

generating a first string through application of ~~applying~~ a one-way hash function ~~on~~ to the n-bit raw number with a first secret key ~~to generate a first string~~;

designating a m-bit portion of the first string as an m-bit validation number;

generating a second string by combining the m-bit validation number and the n-bit raw number ~~to generate a second string~~;

generating a third string through application of~~applying~~ a DES3 encryption algorithm to the second string with a second ~~secet~~ secret key ~~to generate a third string~~; and

producing the code with the encrypted information by converting the third string to a base L string~~to generate the code with the encrypted information~~.

10. (Currently Amended) The method of claim ~~9~~1, wherein the decryption of the base 2 string is performed through application of a reverse DES3 encryption algorithm with the second secret key which produces a second test code, and wherein the step of verifying further includes ~~the steps of:~~

~~converting the code in base L to generate a first test code in base 2;~~

~~decrypting the first test code with the second secret key using a reverse DES3 encryption algorithm to generate a second test code;~~

generating a third test code through application of~~applying~~ the one-way hash algorithm to the second test code~~to generate a third test code;~~ and

comparing a designated m-bit portion of the second test code to a designated m-bit portion of the third test code~~,~~ and declaring the code valid if the comparison is positive~~, declaring the code to be valid~~.

11. (Original) The method of claim 10, wherein the m-bit validation number is the m-most significant bit (MSB) of the first string in the generating step and the designated m-bit portion is the most significant bit portion of the second test code in the comparing step.

12. (Currently Amended) A method for awarding incentive points to a user, comprising the steps of:

~~generating a code with encrypted information;~~

~~providing the code to an entity for printing on an object;~~

receiving on-line~~the code~~ from a user ~~on line, the~~ a code ~~having been~~ generated with encrypted information and obtained by the user off-~~reterived from the object by the user~~;

verifying the validity of the code by processing the encrypted information; and

awarding incentive points to the user if the code is valid.

13. (Currently Amended) The method of claim 12, wherein the code is generated by~~step of generating includes the steps of~~:

providing an n-bit raw number;

generating a first string through application of~~applying~~ a one-way hash function ~~on~~ to the ~~en-bit~~n-bit raw number with a first secret key~~to generate a first string~~;

designating an m-bit portion of the first string as an m-bit validation number;

generating a second string through combination of~~combining~~ the m-bit validation number and the n-bit raw number~~to generate a seond string~~;

generating a third string through application of~~applying~~ a DES3 encryption algorithm to the second string with a second secret key~~to generate a third string~~; and

producing the code with the encrypted information through conversion of~~converting~~ the third string to a base L string~~to generate ateh code with the encrypted information~~.

14. (Currently Amended) The method of claim ~~13~~12, wherein the step of verifying includes:

generating a first test code by converting the ~~code in~~ base L string of the code to a base 2 string~~generate a first test code in base 2~~;

generating a second test code by decrypting the first test code with the second secret key using a reverse DES3 encryption algorithm~~ to generate a second test code~~;

generating a thirst test code by applying the one-way hash algorithm to the second test code~~ to generate a third test code~~; and

determining the validity of the code by comparing a designated m-bit portion of the second test code to a designated m-bit portion of the third test code~~, and if the comparison is positive, declaring the code to be valid~~.

15. Canceled

16. (Currently Amended) The method of claim ~~15~~14, wherein the m-bit validation number is the m most significant bit (MSB) of the first string in the generating step and the designated m-bit portion is the most significant bit portion of the second test code and third test code in the comparing step.

17. (Currently Amended) An offline-online points system, comprising:

a main server configured ~~for providing a user~~ with an interface ~~to~~ for ~~submit~~ receiving a code from a user, wherein the code is obtainable by the user ~~offline~~off-line and is associated with N points, wherein each point, characterized as a purchase or attention incentive point, is redeemable and maintainable in an account for the user; and

a code server configured for maintaining valid codes and verifying, against the valid codes, the validity of ~~that~~ the code ~~submitted by~~received from the user, wherein the account has a balance of points capable of growing~~ is valid such that a balance in the account for the user is increased~~ by a predetermined number of points if the code is valid.;

~~means for generating the code; and~~

~~means for fixing the code onto a medium such that the code is obtainable from the medium offline.~~

18. (Currently Amended) The ~~offline online points system~~method of claim ~~17~~12, wherein the code is generated by:~~wherein the means for generating the code includes~~

~~means for~~ providing a number portion,

~~means for~~ deriving a validation portion from the number portion,

~~means for~~ appending the validation portion to the number portion to form a string,

~~means for~~ encrypting the string, and

~~means for~~ deriving the code from the encrypted string by converting the encrypted string to base L string.

19. (Currently Amended) The ~~offline-online points system~~method of claim 18, wherein the code is a fixed-length string with C characters, and wherein the ~~means for~~step of deriving the code further includes ~~means for~~ prepending a character to the base L string any number of times that is needed to achieve the fixed-length of C characters.

20. (Currently Amended) The ~~offline-online points system~~method of claim 18, wherein L is the number of characters in the alphabet.

21. (Currently Amended) The ~~offline-online points system~~method of claim 18, wherein the string is 48-bits long and the number portion is 32-bits long.

22. (Currently Amended) The ~~offline-online points system~~method of claim ~~17~~12, wherein the code is generated by:~~wherein the means for generating the code includes~~

~~means for~~ providing a number portion, $S1_{INT}$, from a first string, S1

~~means for~~ arranging a first secret key, K1, next to the number portion, $S1_{INT}$, from S1, to form a second string, S2,

~~means for~~ applying a hash function to S2 to produce a third string, S3,

~~means for~~ extracting a validation portion, $S1_{VAL}$, from S3 and arranging $S1_{VAL}$, next to $S1_{INT}$ in S1 ($S1=S1_{VAL}+ S1_{INT}$),

~~means for~~ encrypting S1 using a second secret key, K2, to form a fourth string, S4, and

~~means for~~ deriving the code by converting S4 to a base L fixed-length code string.

23. (Currently Amended) The ~~offline-online points system~~method of claim 22, wherein the first and second secret keys, K1 and K2, are 128-bits long and the encryption ~~means~~ includes DES3 encryption algorithm.

24. (Currently Amended) The ~~offline-online points system~~method of claim 22, wherein the hash function ~~application means has~~ includes MD5, a one-way hash algorithm.

25. (Currently Amended) The ~~offline-online points system~~method of claim 22, wherein S1 is 48-bits long and the number portion, $S1_{INT}$, is 32-bits long.

26. (Currently Amended) The offline-online points system of claim 17, wherein for verifying the ~~submitted~~ code received from the user the code server includes:~~,~~

means for converting the ~~submitted~~ code from a base L string into a base 2 string, $S4_{BASE2}$;~~,~~

means for decrypting $S4_{BASE2}$ using a second secret key, K2, to form a decrypted first string, S1';~~,~~

means for providing a number portion, $S1'_{INT}$, from S1';

means for arranging a first secret key, K1, next to the number portion, $S1'_{INT}$, from S1, to form a second string, S2';~~,~~

means for applying a hash function to S2' to form a third string S3'~~,~~;

means for extracting a validation portion from S3' and a validation portion from S1'~~,~~; and

means for determining if the code is valid by comparing the validation portion from S3' with the validation portion from S1'.

27. (Original) The offline-online points system of claim 26, wherein S3' and S1 are each 48-bits long and the secret keys, K1 and K2 are 128-bits long.

28. (Currently Amended) The offline-online points system of claim 26, wherein the decryption means includes $DES3^{-1}$ decryption algorithm means and the hash function application means includes MD5 hash algorithm means.

29. (Currently Amended) A method for offline-online ~~handling~~ management of incentive points, comprising:

receiving ~~generating~~ a code~~, wherein wherein the code is~~ generated by providing a number portion, deriving a validation portion from the number portion, appending the validation portion to the number portion to form a string, encrypting the string, and deriving the code from the encrypted string by converting the encrypted string to base L string, the code obtained off-line and received on-line; and

processing the code.

~~fixing the code onto a medium such that the code is obtainable from the medium offline~~.

30. (Currently Amended) The method of claim 29, ~~further comprising~~wherein processing the code includes:

~~obtaining the code offline;~~

submitting the code ~~online~~ to a server that has valid codes, wherein the code is associated with N points maintained by the server in a user account, wherein each point, characterized as a purchase or attention incentive point, is redeemable; and

verifying the ~~submitted~~ code against the valid codes to determine if it is valid, wherein if the ~~submitted~~ code is valid, a predetermined number of points are added to the user account.

31. (Original) A method as in claim 29, wherein the code is a fixed-length string with C characters, and wherein a character is prepended to the base L string any number of times that is needed to achieve the fixed-length of C characters.

32. (Original) A method as in claim 29, wherein L is the number of characters in the alphabet.

33. (Original) A method as in claim 29, wherein the string is 48-bits long and the number portion is 32-bits long.

34. (Currently Amended) A method for offline-online ~~handling~~ management of incentive points, comprising:

generating a code by:

providing a number portion, $S1_{INT}$, from a first string, S1,

arranging a first secret key, K1, next to the number portion, $S1_{INT}$, from S1, to form a second string, S2,

applying a hash function to S2 to produce a third string, S3,

extracting a validation portion, $S1_{VAL}$, from S3 and arranging $S1_{VAL}$, next to $S1_{INT}$ in S1 ($S1=S1_{VAL}+ S1_{INT}$),

encrypting S1 using a second secret key, K2, to form a fourth string, S4, and

deriving the code by converting S4 to a base L fixed-length code string; and

fixing the code onto a medium such that the code is obtainable from the medium ~~offline~~off-line.

35. (Currently Amended) A method as in claim 34, wherein the first and second secret keys, K1 and K2, are 128-bits long and the encryption involves a DES3 encryption algorithm.

36. (Original) A method as in claim 34, wherein the hash function is MD5, a one-way hash algorithm.

37. (Original) A method as in claim 34, wherein S1 is 48-bits long and the number portion, $S1_{INT}$, is 32-bits long.

38. (Original) A method as in claim 30 wherein the step of verifying the submitted code includes,

converting the submitted code from a base L string into a base 2 string, $S4_{BASE2}$,

decrypting $S4_{BASE2}$ using a second secret key, K2, to form a decrypted first string, S1',

providing a number portion from S1'

arranging a first secret key, K1, next to the number portion from S1' to form a second string, S2',

applying a hash function to S2' to form a third string S3',

extracting a validation portion from S3' and a validation portion from S1', and

determining if the code is valid by comparing the validation portion from S3' with the validation portion from S1'.

39. (Original) A method as in claim 38, wherein S3' and S1 are each 48-bits long and the secret keys, K1 and K2 are 128-bits long.

40. (Currently Amended) A method as in claim 38, wherein the decryption involves the $DES3^{-1}$ decryption algorithm and the ~~has~~ hash function involves the MD5 hash algorithm.